(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 644 084**

(51) Int. CI.:

H04W 12/06 (2009.01)
H04W 4/00 (2009.01)
H04L 9/08 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **08.07.2014 PCT/EP2014/064618**

(87) Fecha y número de publicación internacional: **26.02.2015 WO15024702**

(96) Fecha de presentación y número de la solicitud europea: **08.07.2014 E 14736822 (9)**

(97) Fecha y número de publicación de la concesión europea: **17.05.2017 EP 3036927**

(54) Título: **Objetivo de comunicación sin contacto capaz de comunicar con un lector NFC**

(30) Prioridad:

20.08.2013 EP 13306158

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
27.11.2017

(73) Titular/es:

GEMALTO SA (100.0%)
6 Rue de la Verrerie
92190 Meudon, FR

(72) Inventor/es:

DANY, VINCENT y
MOURTEL, CHRISTOPHE

(74) Agente/Representante:

CASANOVAS CASSA, Buenaventura

DESCRIPCIÓN

Objeto de comunicación sin contacto capaz de comunicar con un lector NFC.

Campo de la invención

La presente invención se refiere a un objeto de comunicación sin contacto capaz de comunicarse con un lector NFC. Más particularmente, la invención se refiere a un objeto de este tipo que dispone de varios contenedores virtuales que tienen una estructura de memoria común con al menos un mismo sector de memoria destinado a ser accedido por lectores asociados a diferentes servicios. Cada uno de tales sectores de memoria tiene al menos una clave asociada al servicio correspondiente.

Más precisamente, la invención se refiere a dicho objeto cuando está destinado a recibir, del lector NFC, información de sector de memoria sobre el sector de memoria a acceder y datos de inicialización dependiendo de la clave del servicio correspondiente a este lector NFC. Dicho objeto incluye un módulo de autenticación para utilizar la clave asociada al servicio correspondiente a un lector NFC para realizar la autenticación con la clave apropiada y los datos almacenados en el contenedor virtual apropiado.

La invención se refiere también a un método para determinar un sector de memoria en un objeto de comunicación sin contacto capaz de comunicarse con un lector NFC de la invención.

Antecedentes de la invención

La invención se refiere al contexto M4M de Mifare4Mobile. Esta solución permite tener múltiples proveedores de servicios Mifare en una sola UICC NFC. Varias imágenes potencialmente activas están presentes en un único objeto de comunicación como visible desde el lector NFC. Cada imagen tiene las mismas funcionalidades en relación con una aplicación raíz que responde al lector NFC que el objeto está bajo el estándar Mifare.

Sin embargo, la solución M4M no define la manera de seleccionar la tarjeta virtual correcta. Las soluciones actuales conocidas para esta selección incluyen las que son completamente manuales. Aquí, el usuario final elige de forma manual la tarjeta virtual gracias a un monedero móvil. También comprende soluciones que requieren una modificación por infrarrojos. Aquí se utilizan los datos de detección de área Wi-Fi, lectura de etiquetas o localización geográfica. Sin embargo, la precisión no es satisfactoria en algunos casos y no cubre situaciones en las que el lector NFC no tiene localización definida (por ejemplo, en un bus). Además, todos estos métodos de selección no funcionan si la batería del teléfono está agotada. Por ejemplo, significa que un usuario final con la batería agotada no podría atravesar el torniquete para tomar el metro.

En particular, la EP 2626823 describe una aplicación monedero en un terminal móvil adaptada para reconocer la localización geográfica del dispositivo terminal móvil independientemente de cualquier presencia de lector de campo de comunicación externo cercano y de cualquier interacción de usuario y en respuesta a la localización geográfica reconocida para seleccionar automáticamente una de las aplicaciones de tarjeta aceptables para el sistema de aceptación de tarjetas asociadas en esa localización geográfica como una aplicación de tarjeta por defecto o en caso de múltiples aplicaciones de tarjeta aplicables en esa localización geográfica para mostrar una lista de aplicaciones de tarjeta aplicables para permitir la selección a un usuario del dispositivo terminal móvil.

La WO 2009/144612 revela un mecanismo para el acceso rápido y seguro a aplicaciones MIFARE instaladas en una memoria MIFARE (un único receptáculo). Un lector NFC asociado a una aplicación MIFARE particular que detecta un dispositivo de comunicación móvil dentro de su cobertura, busca un sector S y una clave K asociada a la aplicación MIFARE particular e inicia la lectura del sector S de la memoria MIFARE del dispositivo de comunicación móvil con la clave correcta K.

Para el problema de la batería agotada, una solución consistiría en modificar la aplicación Mifare4Mobile para definir una tarjeta virtual predeterminada que se seleccionará automáticamente cuando la batería esté vacía. Sin embargo, es una solución parcial que funciona sólo para trayectos más regulares y que es aplicable sólo para un proveedor de servicios. Por ejemplo, permite tomar el autobús pero no la entrada en un edificio de oficinas.

Por consiguiente, serían deseables, en el estado de la técnica, otras soluciones alternativas y ventajosas.

Sumario de la invención

La presente invención tiene por objeto permitir la elección del contenedor virtual en cualquier momento sin la interacción del usuario final, al menos en el contexto Mifare4Mobile.

Para este propósito, la presente invención se refiere a un objeto de comunicación sin contacto que comprende:

- un módulo de cálculo destinado a calcular diferentes datos de prueba posibles utilizando claves asociadas al sector de memoria indicadas en la información del sector de memoria para cada uno de los contenedores virtuales,

- un módulo de detección de coincidencia para detectar la coincidencia de los datos de inicialización recibidos del lector NFC con uno de los datos de prueba calculados localmente.

tomando entonces, el módulo de autenticación, la clave correspondiente a los datos de prueba coincidentes, si se detectan alguna vez, para realizar la autenticación.

La solución de acuerdo con la invención es así automática y fácil de usar. De hecho, no requiere ninguna acción manual para seleccionar la tarjeta virtual. La solución es. Asimismo, rentable y fácil de desplegar porque no hay necesidad alguna de modificación ni en el lector NFC ni en el sistema de back-end del proveedor de servicios. Además, la solución aumenta la fiabilidad al 100% porque funciona incluso cuando la batería del teléfono se encuentra agotada. Con esta invención, la idea es así seleccionar automáticamente en la aplicación M4M la tarjeta virtual correcta en el momento en que el teléfono se presenta delante del lector NFC.

De acuerdo con la implementación preferida, el objeto de comunicación sin contacto pertenece al grupo formado por la tarjeta UICC NFC, eSE, UICC NFC emulada en un procesador de aplicación.

Estas implementaciones permiten proporcionar un nivel satisfactorio de seguridad en la autenticación, las soluciones más seguras son tarjetas UICC NFC o elementos seguros integrados (eSE). Sin embargo, en la aplicación Mifare4Mobile, el microcontrolador del

teléfono inteligente podría emular una UICC NFC mientras mantiene un nivel de seguridad razonable.

Ventajosamente, el objeto de comunicación sin contacto es del tipo Mifare Clásico.

Esto se corresponde con la aplicación preferida para la invención.

La presente invención se refiere también a un dispositivo de comunicación que tiene un objeto de comunicación sin contacto de acuerdo con la invención.

La invención se refiere también a un método para determinar un sector de memoria en un objeto de comunicación sin contacto capaz de comunicarse con un lector NFC, teniendo dicho objeto varios contenedores virtuales que tienen una estructura de memoria común con al menos un mismo sector de memoria destinado a ser accedido por lectores NFC asociados a diferentes servicios, teniendo cada uno de dichos sectores de memoria al menos una clave asociada al servicio correspondiente, comprendiendo dicho método las etapas de:

recepción, de un lector NFC, de una información de sector de memoria sobre el sector de memoria a acceder y datos de inicialización dependiendo de la clave del servicio correspondiente a este lector NFC,

autenticación utilizando la clave asociada al servicio correspondiente a un lector NFC y datos almacenados en un contenedor virtual apropiado.

caracterizado dicho método porque incluye además etapas de:

- cálculo de diferentes datos de prueba posibles usando claves asociadas al sector de memoria indicadas en la información del sector de memoria para cada uno de los contenedores virtuales.

- detección de coincidencia que detecta la coincidencia de los datos de inicialización recibidos del lector NFC con uno de los datos de prueba calculados localmente.

la etapa de autenticación tomando entonces la clave correspondiente a los datos de prueba coincidentes, si se detectan alguna vez, para realizar la autenticación.

Tal método implementado en el dispositivo de comunicación sin contacto permite una selección automática del contenedor virtual sin necesidad de ningún cambio en los lectores NFC o por parte del proveedor de servicios.

De acuerdo con una característica específica, la etapa de cálculo de diferentes datos de prueba posibles utilizando claves asociadas al sector de memoria indicado en la información de sector de memoria para cada uno de los contenedores virtuales utiliza elementos calculados preliminarmente.

Esta característica permite acelerar los cálculos.

De acuerdo con una característica ventajosa, la etapa de calcular diferentes datos de prueba posibles utilizando claves asociadas al sector de memoria indicado en la información de sector de memoria para cada uno de los contenedores virtuales utiliza un histórico de los contenedores coincidentes.

Esto permite acelerar la coincidencia evitando calcular el conjunto completo de posibilidades en una situación específica. En particular, permite calcular primero el último contenedor coincidente históricamente y luego los demás. Si el usuario no se ha movido, la coincidencia será más rápida. Para la realización de los finales precedentes y relacionados, una o más realizaciones comprenden las características que se describen en adelante y que se señalan particularmente en las reivindicaciones.

Breve descripción de los dibujos

La siguiente descripción y los dibujos adjuntos plasman en detalle ciertos aspectos ilustrativos y son indicativos de algunas de las diversas maneras en que pueden emplearse los principios de las realizaciones. Otras ventajas y características novedosas se pondrán de manifiesto a partir de la siguiente descripción detallada cuando se considere en conjunción con los dibujos y las realizaciones descritas pretenden incluir todos estos aspectos y sus equivalentes.

- La Figura 1 muestra esquemáticamente un contexto en el que la invención es implementada ventajosamente;

- La Figura 2 representa esquemáticamente el contenido de un objeto de comunicación sin contacto de la invención;

- La Figura 3 muestra un diagrama de flujo esquemático del método de la invención.

Descripción detallada de realizaciones de la invención

Los mismos elementos han sido designados con los mismos números de referencia en los diferentes dibujos. Para mayor claridad, sólo se han mostrado en los dibujos aquellos elementos y etapas que son útiles para la comprensión de la presente invención y serán también descritos.

La FIG. 1 muestra esquemáticamente un contexto en el que la invención se implementa de forma ventajosa. Comprende un dispositivo de comunicación 1 que tiene en su interior un objeto de comunicación sin contacto 10 del tipo al que se aplica la presente invención como una realización.

Dado que comprende el objeto de comunicación sin contacto 10, el dispositivo de comunicación 1 es capaz de comunicarse con un lector NFC 2. Para este fin, también comprende una interfaz sin contacto CLF, conectado por sí mismo a al menos una aplicación APP y al objeto de comunicación sin contacto 10. Esta conexión es, por ejemplo, de acuerdo con una tecnología conocida que comprende al menos una línea de alimentación Vcc y una línea de datos DL. También concierne a otras implementaciones en las que se emularía el objeto de comunicación sin contacto en el propio dispositivo de comunicación. En este último caso, el protocolo de conexión sería diferente pero también conforme con la tecnología conocida en el campo.

Debe tenerse en cuenta aquí que la interfaz sin contacto CLF está aquí representada dentro del dispositivo de comunicación 1, pero también se puede implementar dentro del propio objeto de comunicación sin contacto. Esto se refiere en particular a la tarjeta micro SD totalmente sin contacto que se despliega en la banca móvil. Esos dispositivos tienen integrados CLF propios. En este último caso, el objeto de comunicación sin contacto 10 es independiente y capaz de comunicarse directamente con un lector 2.

El objeto de comunicación sin contacto 10 tiene varios contenedores virtuales C1, C2, C3 que tienen una estructura de memoria común 110/120/130, 210/220/230, 310/3201330 con al menos un mismo sector de memoria 120, 220, 320 destinado a ser accedido los lectores NFC 2 asociados a diferentes servicios. Típicamente, esta situación se da cuando varios servicios de transporte público son dirigidos por el dispositivo de comunicación sin contacto.

Por ejemplo, el usuario se ha registrado en París, Londres y Berlín para el transporte público. Tan pronto como los lectores NFC recurren al mismo sector de memoria en cualquiera de esos lugares, aparece el problema resuelto por la invención.

De hecho, actualmente no existe un medio para seleccionar el sector de memoria correcto en uno de los tres contenedores C1, C2, C3 excepto utilizando entradas externas como preguntar al usuario a través de una pantalla de visualización o datos de geolocalización.

El contexto de la invención es tal que cada uno de tales sectores de memoria 120, 220, 320 tiene al menos una clave K1, K2 y K3 asociada al servicio correspondiente. Esta clave tiene que ser utilizada para proceder a la necesaria autenticación del objeto 10 con el lector NFC 2.

Por ejemplo, el contenedor C1 contiene datos de control de acceso de usuario 110, datos del transporte público de Paris 120 y datos de fidelización del supermercado A 130. El contenedor C2 contiene los datos de fidelización 212 del supermercado B y los datos del transporte público de Londres 220. Finalmente, el contenedor C3 contiene datos de control de acceso de usuario 310, datos del transporte público de Berlín 320 y datos de fidelización del cine 330.

Cualquier solicitud de autenticación del lector NFC 2 del transporte público comprende información de sector de memoria MSI que designa el sector de memoria a utilizar para la autenticación y la identificación de datos ID para permitir que se realice la autenticación.

Tal como se simboliza mediante la flecha, la información del sector de memoria MSI dirige siempre al mismo sector de memoria, cualquiera que sea del contenedor C1, C2, C3. No existe ningún medio para que el objeto de comunicación sin contacto 10 sepa cuál de los tres sectores de memoria correspondiente en cada uno de los contenedores C1, C2, C3 está afectado por la solicitud de autenticación del lector NFC 2 y, por tanto, qué clave asociada ha de usarse.

La figura 2 muestra esquemáticamente el contenido de un objeto de comunicación sin contacto de la invención. Comprende un módulo de cálculo 11 capaz de leer en los diferentes contenedores las claves K1, K2, K3 en sectores de memoria como se indica en la información de sector de memoria. Las claves de lectura se utilizan para calcular diferentes datos de prueba posibles TDi, i = 1 a 3 aquí

Estos datos de prueba TDi se proporcionan como entrada a un módulo de detección de coincidencia 12 para detectar la coincidencia de los datos de inicialización ID recibidos del lector NFC 2 con uno de los datos de prueba calculados localmente TDm.

El objeto de comunicación sin contacto incluye un módulo de autenticación 13 que toma la clave correspondiente a los datos de prueba de coincidencia TDm, si se detecta alguna vez, para realizar la autenticación.

La Figura 3 muestra un diagrama de flujo del método de la invención tal como se implementa en un objeto de comunicación sin contacto de la invención. En una primera etapa E1, se recibe la información del sector de memoria sobre el sector de memoria a ser accedido y los datos de inicialización dependiendo de la clave del servicio correspondiente a este lector NFC de un lector NFC.

Antes de esta recepción o posteriormente, se realiza una etapa E2 de cálculo de diferentes datos de prueba posibles TDi usando claves Ki asociadas al sector de memoria indicado en la información del sector de memoria MSI para cada uno de los contenedores virtuales. Cuando esta etapa no se realiza por defecto desde el sector de memoria similar diferente, sino sólo una vez que se recibe una solicitud de un lector NFC, se proporciona la información de sector de memoria MSI para el cálculo de la etapa E2. Esto se muestra en línea discontinua en la figura 3.

En una etapa E3, la detección de coincidencia que detecta la coincidencia de los datos de inicialización ID recibidos del lector NFC 2 con un TDm de los datos de prueba calculados localmente TDi.

Esta etapa permite proporcionar la clave correcta Km correspondiente a los datos de prueba de coincidencia TDm a una etapa de autenticación E4. Esta etapa de autenticación consiste en realizar un proceso de autenticación conocido utilizando la clave de coincidencia Km. Esto puede resultar en un rechazo REF o en una autenticación AUTH del par lector/objeto NFC.

Más precisamente, cuando el contexto Mifare4Mobile es dirigido por la invención, la tarjeta analizara el criptograma enviado por el lector durante la autenticación para seleccionar la tarjeta virtual correcta.

De hecho, el objeto de comunicación sin contacto, aquí una tarjeta, incluye un generador de números aleatorios para generar un reto nounce enviado por la etiqueta de manera clara. Por lo tanto, en ese momento aún no es necesaria la clave para la autenticación.

El lector NFC asociado con un servicio suministrado por un proveedor de servicios dado, procede entonces a un proceso de autenticación. Durante esta operación, dicho reto nounce sirve para que el lector NFC pueda calcular un criptograma usando al menos una clave asociada al servicio dado. Para este propósito, dicho lector NFC tiene un banco de claves que incluye la clave de etiqueta.

Este criptograma se envía entonces a la tarjeta. El servicio accedido dependerá así de la información dada por el lector NFC.

Al recibir la respuesta del lector NFC que comprende un criptograma calculado a partir del nounce entre otros, la tarjeta puede calcular todos los posibles criptogramas posibles para cada tarjeta virtual. Permite establecer cuál fue utilizado por el lector NFC y finalmente terminar la autenticación con la clave adecuada.

La invención permite así proporcionar una UICC NFC que tiene múltiples proveedores de servicios Mifare y medios para seleccionar uno u otro de forma automática y fiable.

Con la invención, la selección es siempre posible incluso en el caso de que la batería esté agotada porque los cálculos requeridos pueden realizarse tan pronto como la tarjeta esté en el campo de un lector NFC. El suministro es del tipo "poder por el campo".

En la descripción detallada anterior, se hace referencia a los dibujos adjuntos que muestran, a modo ilustrativo, realizaciones específicas en las que la invención puede ser practicada. Estas realizaciones se describen con suficiente detalle para permitir practicar la invención a los expertos en la técnica. Debe entenderse que la ubicación o disposición de elementos individuales dentro de la realización descrita puede ser modificada sin apartarse del espíritu y alcance de la invención. Por lo tanto, la descripción anteriormente detallada no debe tomarse en un sentido limitativo, y el alcance de la presente invención está definido únicamente por las reivindicaciones adjuntas.

REIVINDICACIONES

1. Objeto de comunicación sin contacto (10) capaz de comunicarse con un lector NFC (2), teniendo dicho objeto (10) varios contenedores virtuales (C1, C2, C3) que tienen una estructura de memoria común con al menos un mismo sector de memoria (120, 220, 320) estando pensado para ser accedido por lectores NFC (2) asociados al servicio correspondiente,

estando destinado dicho objeto (10) a recibir, de un lector NFC (2), información del sector de memoria (MSI) sobre el sector de memoria a acceder y datos de inicialización (ID) dependiendo de la clave del servicio correspondiente a este lector NFC (2),

incluyendo dicho objeto (10) un módulo de autenticación (13) para utilizar la clave (Km) asociada al servicio correspondiente a un lector NFC (2) para realizar la autentificación con la clave apropiada (Km) y los datos almacenados en el contenedor virtual apropiado (Cm),

dicho objeto (10) estando **caracterizado** porque incluye además·

- un módulo de cálculo (11) pensado para calcular diferentes datos de prueba posibles (TDi, i = 1 a 3) utilizando las claves (K1, K2, K3) asociadas al sector de memoria indicado en la información de sector de memoria (MSI) para cada uno de los contenedores virtuales (C1, C2, C3).

- un módulo de detección de coincidencia (12) para detectar la coincidencia de los datos de inicialización (ID) recibidos del lector NFC (2) con uno de los datos de prueba calculados localmente (TDi),

el módulo de autenticación (13) tomando entonces la clave (Km) correspondiente a los datos de prueba de coincidencia (TDm), si se detecta alguna vez, para realizar la autenticación.

2. Objeto de comunicación sin contacto como se reivindica en la reivindicación 1, que pertenece al grupo formado por la tarjeta UICC NFC, eSE, UICC NFC emulada en un procesador de aplicación.

3. Objeto de comunicación sin contacto como se reivindica en la reivindicación 1, que es del tipo Mifare Clásico.

4. Dispositivo de comunicación (1) que incorpora un objeto de comunicación sin contacto (10) de acuerdo con una de las reivindicaciones precedentes.

5. Método para determinar un sector de memoria en un objeto de comunicación sin contacto (10) capaz de comunicarse con un lector NFC (2), teniendo dicho objeto (10) varios contenedores virtuales (C1, C2, C3) que tienen una estructura de memoria común con al menos un mismo sector de memoria estando pensado para ser accedido por lectores NFC (2) asociados a diferentes servicios, cada uno de dichos sectores de memoria teniendo al menos una clave (K1, K2, K3) asociada al servicio correspondiente, comprendiendo dicho método las etapas de:

- recepción (E1), de un lector NFC (2), de una información de sector de memoria (MSI) sobre el sector de memoria a acceder y datos de inicialización (ID) dependiendo de la clave del servicio correspondiente a este lector NFC (2),

autenticación (E4) utilizando la clave asociada al servicio correspondiente a un lector NFC y datos almacenados en un contenedor virtual apropiado,

caracterizándose dicho método porque incluye además etapas de:

- cálculo (E2) de diferentes datos de prueba posibles (TDi) utilizando claves asociadas al sector de memoria indicado en la información de sector de memoria (MSI) para cada uno de los containers virtuales (C1, C2, C3),

- detección de coincidencia (E3) que detecta la coincidencia de los datos de inicialización (ID) recibidos del lector NFC (2) con una de los datos de pruebas calculadas localmente (TDi),

la etapa de autenticación (E4) tomando entonces la clave (Km) correspondiente a los datos de prueba coincidentes (TDm), si se detecta alguna vez, para realizar! la autenticación.

6. Método de acuerdo con la reivindicación 5, en el que la etapa de cálculo (E2) de diferentes datos de prueba posibles (TDi, i = 1 a 3) utilizando claves (K1, K2, K3) asociadas al sector de memoria indicado en la información del sector de memoria (MSI) para cada uno de los contenedores virtuales (C1, C2, C3) utiliza elementos calculados preliminarmente.

7. Método de acuerdo con la reivindicación 5, en el que la etapa de cálculo (E2) de diferentes datos de prueba posibles (TDi) utilizando claves asociadas al sector de memoria indicado en la información del sector de memoria para cada uno de los contenedores virtuales (C1, C2, C3) utiliza una histórico de los contenedores coincidentes.

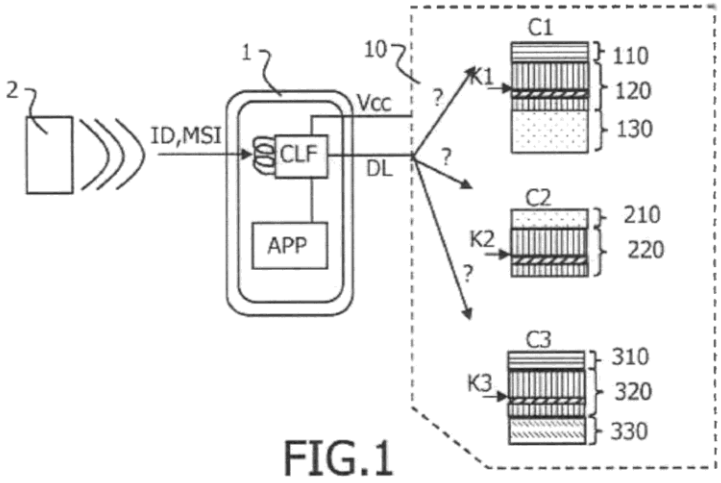

FIG.1

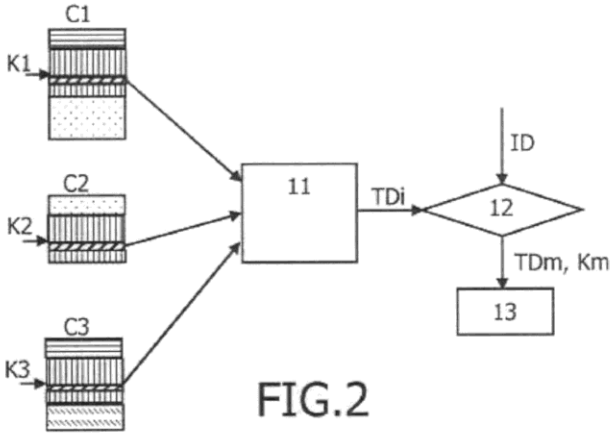

FIG.2

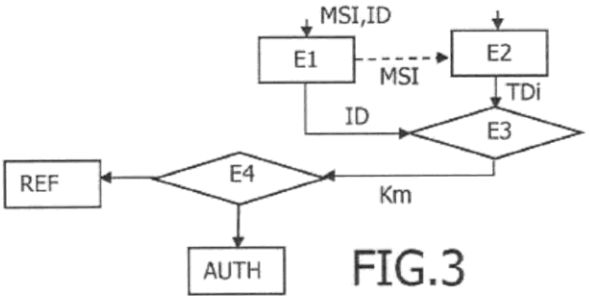

FIG.3